



TARBIJAKAITSE JA
TEHNILISE JÄRELEVALVE
AMET

KÄSKKIRI

08.05.2026 nr 1-2/26-043

Riskihalduse kord

Majandus- ja tööstusministri 30.03.2026 määruse nr 10 „Tarbijakaitse ja Tehnilise Järelevalve Ameti põhimäärus“ § 6 p 1 alusel

1. kinnitan riskihalduse korra (lisatud);
2. tunnistan kehtetuks Tarbijakaitse ja Tehnilise Järelevalve Ameti peadirektori 16.12.2024.a käskkirja nr 1-2/24-078 „Riskijuhtimise kord“.

(allkirjastatud digitaalselt)
Kristi Talving
peadirektor

Koostaja: Mariko Männa

Tarbijakaitse ja Tehnilise Järelevalve Ameti riskihalduse kord

1. Üldpõhimõtted

- 1.1. Riskihalduse korra eesmärk on kehtestada Tarbijakaitse ja Tehnilise Järelevalve Ameti (edaspidi TTJA või amet) teenistujatele ühtsed reeglid riskihalduse korraldamiseks. Riskihaldus toetab ameti eesmärkide saavutamist, vähendab ebakindlusest tulenevaid mõjusid ning kaitseb infosüsteeme, andmeid ja teenuseid nende konfidentsiaalsuse, tervikluse ja käideldavuse seisukohalt.
- 1.2. Kord laieneb kõigile TTJA teenistujatele, praktikantidele, lepingu alusel teenust osutavatele isikutele ja kõigile teistele isikutele, kes osalevad TTJA töös (edaspidi teenistuja) ja kehtib kõikides ameti füüsilistes asukohtades. Käesoleva korra sätteid kohaldatakse ka rakenduste, registrite, andmekogude ja andmebaaside (edaspidi välised rakendused) kasutamise korral, kui vastavate väliste rakenduste kasutamise kordades ei ole sätestatud teisiti.
- 1.3. TTJA riskihalduse kord on kooskõlas ning tugineb järgmistele standarditele ja juhistele:
 - 1.3.1. Eesti infoturbestandard (edaspidi E-ITS)
 - 1.3.2. Infoturbe halduse süsteemide (edaspidi ISMS) standardiperesse kuuluvad standardid, sh ISO/IEC 27000:2020, 27001:2023 ja 27005:2022
 - 1.3.3. ISO 31000:2018
 - 1.3.4. ISO 31073:2022
- 1.4. Riskihalduse tagamisel ja rakendamisel tuleb, nii palju kui võimalik, lähtuda kohustuste lahususe põhimõttest.
- 1.5. Riskihalduse korraldamise eelduseks on, et turvameetmed ei loo absoluutset turvalisust, vaid vähendavad turvariski, st tõenäosust, et andmete terviklus, käideldavus või konfidentsiaalsus saavad kahjustatud. Infosüsteemi turvalisus loetakse piisavaks, kui jääkrisk on ameti jaoks aktsepteeritaval tasemel (võrreldes varade väärtusega ja turvameetmete maksumusega). Kui infosüsteemi funktsionaalsus on ameti tegevuses

kriitilise tähtsusega, infosüsteemi asendus- ja arenduskulud on ebamõistlikult suured või kui varasid ähvardab kõrge risk, viiakse vajadusel läbi detailne riskianalüüs.

- 1.6. TTJA tagab kõikide enda käsutuses olevate varade kaitse vastavalt ohtude realiseerumise tõenäosusele ja kaitstavate varade väärtusele.
- 1.7. TTJA rakendab seadusest tulenevate ja oma pädevuses olevate ülesannete täitmiseks turvameetmeid, mis on majanduslikult põhjendatud ning proportsionaalsed kaitstavate varadega.
- 1.8. TTJA varade liigitamise ja haldamise põhimõtted tulenevad Majandus- ja Kommunikatsiooniministeeriumi käskkirjast „Riigivara valitsemise kord Majandus- ja Kommunikatsiooniministeeriumi valitsemisalas“. Varasid hallatakse riigitöötaja iseteenindusportaalil RTIP, IT-varade (näiteks arvutitöökohateenusega seotud IT-varad) haldamise eest vastutavad välised koostööpartnerid (IT-teenuste pakkujad). Väljast tellitud teenuse puhul on TTJA varad kirjeldatud koostööpartnerite infovarade haldamise süsteemides. Kõikide varade kohta on koostatud varade loend.
- 1.9. TTJA rakendab riskide vähendamiseks Eesti infoturbestandardi (edaspidi E-ITS) turvameetmeid vastavalt äriprotsessidele määratud kaitsetarbele ja E-ITS rakendusjuhendile. Kui mõnda E-ITS turvameedet ei ole võimalik või otstarbekas täita, rakendab TTJA alternatiivseid meetmeid riskide maandamiseks (lisaturvameetmed) või aktsepteerib kirjalikult jääkriskid.
- 1.10. Riskide ülevaatus ja riskitasemete kinnitamine toimub TTJA juhtkonna poolt vähemalt üks kord aastas.

2. Rollid ja vastutus

- 2.1. TTJA juhtkond – peadirektor ja asetäitjad, kinnitavad riskiregistri, võtavad vastu otsuseid riskide maandamiseks ja aktsepteerivad jääkriskid lähtuvalt riskide hindamisest. Riski aktsepteerimiseks või maandamiseks teeb kirjaliku ettepaneku riskiomanik.
- 2.2. Riskiomanikud – tuvastavad riskid oma vastutusvaldkonnas, hindavad ja dokumenteerivad riskid ning rakendavad turvameetmeid.
- 2.3. Kriisivalmiduse ja riskijuht või peadirektori poolt nimetatud isik korraldab riskihalduse korra ning teiste valdkonda reguleerivate kordade väljatöötamise ja iga-aastase ülevaatamise ning vajadusel ajakohastamise, haldab riskiprotsessi ja koordineerib hindamisi.
- 2.4. Teenistujad – järgivad kehtestatud ohjemeetmeid ning teavitavad riskidest ja intsidentidest vastavalt IT-korras sätestatule.

3. Mõisted ja viited

Käesolev kord kasutab E-ITS ja ISO 31073:2022 kohaseid mõisteid ja termineid, mis on kättesaadavad E-ITS kodulehel (<https://eits.ria.ee/et/abimaterjalid/seletav-soonaraamat>) ja/või ISO veebipõhisel lugemisplatvormil (<https://www.iso.org/obp/ui>).

- Risk – määramatuse mõju eesmärkidele, ka ohu võimekus tekitada organisatsioonile kahju.
- Riskitase – tagajärje ja tõenäosuse kombinatsioon.
- Riskinorm (*risk appetite*) – riski suurus või tüüp, mida organisatsioon soovib taotleda või säilitada.
- Jääkrisk – risk, mis jääb pärast riskikäsitlust.
- Tagajärg, ka mõju (*consequence*) – sündmuse tulemus, mis mõjutab eesmärke.
- Tõenäosus (*likelihood*) – millegi juhtumise võimalus.
- Meede (*control*) – abinõu, mis säilitab ja/või muudab riski.
- Infoturvainsident – soovimatu või ootamatu infoturvasündmus(tik), mis võib üsna tõenäoliselt kahjustada organisatsiooni põhitegevust ja ohustada teabe turvalisust.

4. Riskihaldus

- 4.1. Riskihaldus on terviklik, dokumenteeritud ja korduv protsess, mis tagab asutuses asjakohase riskidega tegelemise alustades riskihalduse konteksti ja ulatuse määratlemisest ning lõpetades riskide kaalutlemise, käsitlemise, seire, ülevaatuse ja aruandlusega.
- 4.2. Riskihalduse süsteem määratleb protsessi, rollid ja vastutused. Riskide tuvastamisel kasutab TTJA varapõhist metoodikat, kus riske saab tuvastada ja kontrollida varade, ohtude ja nõrkuste ülevaatusega. Riskide hindamise metoodika põhineb riskide mõju ja tõenäosuse tuvastamisel.
- 4.3. Riski kaalutlemine – kogu riskituvastuse, riskianalüüsi ja riski hindamise protsess tervikuna:
 - 4.3.1. Riskituvastus – toimub riskide kaardistamisega. Eesmärk on leida nõrkused ja ohud, millel on mõju TTJA äriprotsessidele või varadele. Tuvastamisel kasutatakse E-ITS etalonturbe alusohtude kataloogi. Riskide loetelus esitatakse riskide informatsioon koos tuvastatud nõrkuste ja ohtudega.

- 4.3.2. Riskianalüüs – protsess riski iseloomu väljaselgitamiseks ja riskitaseme määramiseks. Tuvastatud riskidele määratakse kaalukus riskimaatriksi abil. Riskianalüüsiga määratakse riskisündmustele astmelised hinnangud skaalal:
- a) tõenäosus – harv, keskmine, sage ja väga sage;
 - b) tagajärg (mõju) – madal, keskmine, kõrge ja kriitiline.
- Riskitase arvutatakse tõenäosuse ja tagajärje (mõju) kombinatsioonina ning väljendatakse riskimaatriksi abil leitud kaalukuse hinnanguga – madal, keskmine, kõrge ja väga kõrge. TTJA riskinorm on võrdne riskitasemega “madal”.
- 4.3.3. Riski hindamine – riskianalüüsi tulemite ja riski kriteeriumite võrdlemise protsessi eesmärk on teha kindlaks, kas risk ja/või selle suurus on aktsepteeritav või talutav. TTJA koostab riskide loetelu koos riskiomaniku otsusega riski käsitlemise viisi kohta. Vajadusel määratakse riskide käsitlemise prioriteet.
- 4.4. Riskikäsitus – riski muutmise või säilitamise protsess, mis tegeleb iga riskiga eraldi ning määrab meetmed kahju vähendamiseks. Riskikäsitusviisideks on:
- 4.4.1. riski säilitamine – riski või jääkriski täiendav maandamine pole vajalik, (jääk)riski riskitaseme skoor on riskinormi piires (madal) ja (jääk)risk aktsepteeritakse sellel tasemel;
 - 4.4.2. riski vähendamine – vähendatakse mõju tagajärge ja tõenäosust läbi meetmete rakendamise;
 - 4.4.3. riski jagamine – jagatakse riski kolmandate osapooltega, nt kindlustusega;
 - 4.4.4. riski vältimine – riski täielik ennetamine, otsustades mitte alustada või jätkata tegevust, mis tekitab riski.
- 4.5. Riski aktsepteerimine – teadlik otsus võtta konkreetne risk mis ületab TTJAs kehtestatud riskinormi ning erakorraliselt aktsepteeritakse riskiga kaasnev võimalik mõju, kui seda ei ole võimalik või majanduslikult otstarbekas vähendada. Riski aktsepteerimist käsitletakse erandina ja seejuures tagatakse riski pidev seire.
- 4.6. Turvameetmete valimine riskikäsitluseks – riski käsitlemiseks määrab TTJA turvameetmed, mis aitavad riski muutes saavutada riskinormile vastava taseme. Sobiva etalon turbe kataloogi mooduli olemasolul kasutatakse turvameetmete määramisel ka selle kõrgmeetmeid, lähtuvalt infoturbe põhikomponentidest (C-I-A ehk konfidentsiaalsus, terviklus, käideldavus).
- 4.7. Iga turvameetme kulude võrdlus eeldatava kahjuga või otsese väärtusega ja otsus meetme teostuse poolt või vastu – lõplik turvameetmete koosmõju, kulukuse jm aspektide hindamine ning jääkriskide aktsepteerimine toimub etalon turbe protsessis turvameetmete kinnitamise sammus.

- 4.8. Turvameetmete rakendamine – soovitud riskitaseme saavutamiseks võib olla tarvilik rakendada rohkem kui ühte turvameedet (nt võib ka tuvastatud riski taseme astet vähendada). Kõige otstarbekamaks võib erandjuhtudel osutuda riski säilitamine samal tasemel.
- 4.9. TTJA rakendab etalonturbe põhimõtteid ja kasutab etalonturbe kataloogi määratud turvameetmeid varade kaitseks. Juhul kui etalonturbe kataloogis puudub sobiv moodul või kui kataloogi meetmed ei ole varade kaitsetarbe ja turvaeesmärkide saavutamiseks piisavad, viiakse läbi etalonturbe väline riskihaldus.
- 4.10. Etalonturbe välisesse riskihaldusse suunatakse varad, mille puhul on täidetud vähemalt üks järgmistest tingimustest:
 - 4.10.1. sihtobjekti kaitsetarve on suur või väga suur;
 - 4.10.2. sihtobjekti kaitsetarve on määramata või ebaselge;
 - 4.10.3. sihtobjekti kasutusviis ei vasta etalonturbe kataloogi moodulite kirjeldustele;
 - 4.10.4. etalonturbe kataloogi meetmed osutuvad turvaeesmärkide saavutamisel ebapiisavaks ning jäärisk ei ole aktsepteeritav;
 - 4.10.5. sihtobjektist sõltub samaaegselt mitme organisatsiooni jaoks olulise äriprotsessi toimimine.
- 4.11. Etalonturbe väline riskihaldus viiakse läbi süstemaatilise protsessina, mille eesmärk on tuvastada, hinnata ja käsitleda riske, mida etalonturbe standardmeetmed ei kata või mille puhul standardmeetmete rakendamine ei ole võimalik.
- 4.12. Etalonturbe välise riskihalduse protsess hõlmab vähemalt järgmisi etappe:
 - 4.12.1. sihtobjekti, kaitstavate väärtuste ja eelduste kirjeldamine;
 - 4.12.2. ohtude ja nõrkuste tuvastamine, arvestades sihtobjekti eripära ja kasutuskonteksti;
 - 4.12.3. riskide hindamine, sh riski mõju ja tõenäosuse analüüsimine;
 - 4.12.4. riski käsitlemise otsustamine, sh täiendavate turvameetmete määramine, riski säilitamine, aktsepteerimine, vähendamine, vältimine või jagamine;
 - 4.12.5. rakendatud ja kavandatavate meetmete sobivuse hindamine võrreldes TTJA riskitaluvusega.
- 4.13. Etalonturbe välise riskihalduse käik, asjaolud ja tulemused dokumenteeritakse vastavalt käesolevale korrale.
- 4.14. Etalonturbe väline riskihaldus määrab sihtobjektidele lisaturvameetmeid, lähtudes sihtobjekti kaitsetarbest ja infoturvaeesmärkidest (konfidentsiaalsus, terviklus, kättesaadavus). Vajadusel hinnatakse jääriski aktsepteeritavust ning koostatakse tegevuskava riskide maandamiseks.

- 4.15. Riskide seire ja aruandlus – turvameetmete või käsitusvariantide korrigeerimine käituse vältel. Riske seiratakse perioodiliselt. Seire käigus hinnates ka meetmete efektiivsust ning vajadust täiendavateks riskianalüüsideks.

5. Riskiregister

- 5.1. TTJA dokumenteerib teadaolevad riskid riskiregistris, mida peetakse elektroonilises halduskeskkonnas (Jira), koos ohtude ja nõrkuste tulbaga, millest risk tuleneb.
- 5.2. Riskidest ülevaate saamiseks ning seireks kasutatakse riskiregistrit.
- 5.3. Riskiregistri osaks on riskimaatriks, mille abil tuvastatakse riskitase.
- 5.4. Riskitaseme määramiseks kasutatakse 4x4 riskimaatriksit, mille abil tuvastatakse riskitase (lisa 1).
- 5.5. Riskitasemed ja aktsepteerimise kriteeriumid on:
- 5.5.1. roheline (madal) – Turvameetmed annavad piisava kaitse. Risk / jääkrisk aktsepteeritakse (käsitusviis "riski säilitamine"), kuid ikkagi riski seirates;
- 5.5.2. kollane (keskmine) – Riski võib erakorraliselt aktsepteerida, kui riskile on määratud riski vähendamiseks turvameetmed. Kõrgendatud prioriteediga riski seire;
- 5.5.3. oranž (kõrge) – Vajab sekkumist ja riski vähendamise meetmete lisamist ja rakendamist esimesel võimalusel. Riski võib erakorraliselt aktsepteerida, kui riskile on määratud ja rakendatud turvameetmed. Kõrgendatud prioriteediga riski seire;
- 5.5.4. punane (väga kõrge) – Vajab kohest sekkumist ja riski vähendamise meetmete lisamist ja rakendamist. Vastasel juhul tuleks tegevusest täielikult või osaliselt keelduda.
- 5.6. Vastavalt riskitasemele määratakse riskidele riski käsitusviis (säilitamine, jagamine, vähendamine ja vältimine). Aktsepteeritakse riske, millel on väike mõju või rahaline kulu ning võimalik organisatsioonil taluda. See aitab suunata ressursse kõrgemate riskide maandamiseks.

6. Seire

- 6.1. TTJA seirab riske regulaarselt ja/või sündmuspõhiselt:
- 6.1.1. Madala- ja keskmise tasemega riske seiratakse kord aastas. Kõrge ja väga kõrge tasemega riske kaks korda aastas.

- 6.1.2. Sündmuspõhine riskide seire toimub mh oluliste muudatuste korral (infosüsteemides, varades või protsessides), infoturvaintsidentide toimumisel, uute ohtude või nõrkuste tuvastamisel ning õigusaktide muutumisel.
- 6.2. Riskide seire hõlmab pidevat tagasisidet intsidentidest.
- 6.3. Riskide seiret koordineerib kriisivalmiduse ja riskijuht või peadirektori poolt nimetatud isik, kaasates tegevusse teenistujaid, kes riskidega tegelevad (riskiomanikud ja meetmete rakendajad).
- 6.4. Riske seiratakse, kasutades ameti riskiaruandlust riskiregistris. Kriisivalmiduse ja riskijuht vaatab riske üle perioodiliselt, kuna riski tase võib ajas muutuda ning tuua kaasa vajaduse täiendavaks riskianalüüsiks.
- 6.5. Riskide seire käigus teostatakse:
 - 6.5.1. infoturbemeetmete asjakohastamine ning määratud meetmete efektiivsuse ja vajaduse hindamine;
 - 6.5.2. regulatsioonide perioodiline läbivaatus;
 - 6.5.3. töökeskkonna regulaarne seire;
 - 6.5.4. infoturbe valdkonda või ameti töökeskkonda puudutavatele muudatustele reageerimine;
 - 6.5.5. infoturvaintsidentide analüüs;
 - 6.5.6. auditeerimine.

7. Riskianalüüs

- 7.1. TTJA tegevust kahjulikult mõjutada võivate toimingute ja sündmuste pidevaks hindamiseks teostatakse riskianalüüsi.
- 7.2. Riskianalüüsi läbiviimist koordineerib kriisivalmiduse ja riskijuht või peadirektori poolt nimetatud isik.
- 7.3. Riskianalüüsi tuleb teostada vähemalt üks kord aastas, samuti enne põhimõtteliste muudatuste tegemist IT-keskkonnas ning peale turvaintsidenti toimumist.
- 7.4. Riskianalüüs viiakse läbi vastavalt käesolevale korrale.
- 7.5. TTJA riskianalüüs põhineb ISO standarditel ja E-ITS etalonturbe metoodikal.
- 7.6. Riski vähendamiseks rakendatakse E-ITS turvameetmeid vastavalt äriprotsesside ja/või sihtobjekti kaitsetarbele ja E-ITS rakendusjuhendile.
- 7.7. Riskide puhul hinnatakse selle esinemise tõenäosust, tagajärgede mõju, likvideerimise kulu ja riski maandamise kulu. Maandatakse riskid, mis tõenäoliselt juhtuvad (4-punkti skaalal 2 või enam) või mille tagajärgede mõju likvideerimise kulu on suurem riski

maandamise kulust. Juhtkonna otsusega on lubatud jätta maandamata risk (aktsepteerida riski), mis juhtkonna hinnangul on väikese tõenäosusega (4-punkti skaalal 1) või mille maandamiseks pole asutusel eelarvet. Viimasel juhul kaalutakse alternatiivseid riski vähendamise võimalusi.

8. Kaitsetarve ja selle määramine

TTJA kaitsetarvete määramise protsess on kirjeldatud TTJA infoturvapoliitikas ning äriprotsessidele määratud kaitsetarbed kinnitatakse infoturvapoliitika lisadena.

Lisa 1 Riskimaatriks

nrQW	TÕENÄOSUS			
	1 Harv	2 Keskmine	3 Sage	4 Väga sage
	4 Kriitiline	Kõrge	Kõrge	Väga kõrge
	3 Kõrge	Keskmine	Kõrge	Väga kõrge
	2 Keskmine	Madal	Keskmine	Kõrge
	1 Madal	Madal	Keskmine	Kõrge

Lisa 2 Protsessijoonis

